AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A watermark-based copy management method for digital media copy protection, the method comprising:

receiving an original media data set that includes ~~an original~~ a watermark, said ~~original~~ watermark including watermark type indicating whether ~~the~~ said watermark is original or not, media owner identification information indicating a media owner and a first copy control information for managing and controlling ~~the~~ a media data copying process, ~~the~~ said first copy control information being set to one of "copy freely", ~~"copy for display only",~~ "copy one generation", "copy never", and "no more copies"~~, wherein the first copy control information being set to "copy for display only" is distinguished from others~~;

~~analyzing said first copy control information to determine whether said first copy control information is set to "copy one generation";~~

playing said original media data set only if said first copy control information is set to "copy freely" or "copy one generation";

embedding a player watermark into said played media data set if said first copy control information is set to "copy one generation", said player watermark including a second copy control information set to "no more copies" and player identification information including

model number and unique serial number, wherein the second copy control information is derived from ~~the~~ said first copy control information; and

transferring said player watermark-embedded media data set to an external device.

2. (Canceled)

3. (Previously Presented) The method of claim 1, wherein said player identification information further includes player vendor.

4. (Currently Amended) A watermark-based copy management method for digital media copy protection, the method comprising:

receiving an original media data set that includes ~~an original~~ a watermark, said ~~original~~ watermark including watermark type indicating whether the watermark is original or not, media owner identification information indicating a media owner and a first copy control information for managing and controlling ~~the~~ a media data copying process, ~~the~~ said first copy control information for indicating at least whether ~~a copy of the~~ copying said original media data is permitted;

~~analyzing said first copy control information to determine~~ performing an operation according to whether said first copy control information indicates ~~at least~~ that ~~the copy~~ said copying is permitted; and

~~performing an operation according to a result of analyzing; and~~

embedding a device watermark into said performed media data set ~~when~~ and transferring ~~the~~ said device watermark embedded media data set to an external device, said device watermark including a second copy control information derived from ~~the~~ said first copy control information and a device identification information including model number and unique serial number.

5. (Currently Amended) The method of claim 4, wherein said device identification information is used to detect an origin of ~~the~~ said performed media ~~copy~~ data set, thereby performing a revocation of a compromised device or their key.

6. (Previously Presented) The method of claim 4, wherein said device identification information further includes device name.

7. (Currently Amended) A watermark-based copy management system for digital media copy protection, the system comprising:

a copy control information analyzer analyzing a first copy control information included in ~~an original~~ a watermark embedded into an original media data set, said first copy control information being set to one of "copy freely", ~~"copy for display only",~~ "copy one generation", "copy never", and "no more copies"~~, wherein the first copy control information being set to "copy for display only" is distinguished from others~~, wherein said ~~original~~ watermark

further includes watermark type indicating whether ~~the~~ said watermark is original or not and media owner identification information indicating a media owner;

a playing element playing said ~~original~~ media data set ~~only~~ if said first copy control information is set to "copy freely" or "copy one generation";

a watermark generator embedding a player watermark into said played data set if said first copy control information is set to " copy one generation", said player watermark including a second copy control information set to "no more copies" and player identification information including model number and unique serial number, ~~wherein the~~ said second copy control information is derived from ~~the~~ said first copy control information; and

a recording ~~or displaying~~ device recording ~~or displaying~~ said player watermark-embedded media data set.

8. (Canceled)

9. (Previously Presented) The system of claim 7, wherein said player identification information further includes player vendor.

10. (Currently Amended) A watermark-based copy management system for digital media copy protection, the system comprising:

a copy control information analyzer analyzing a first copy control information included in ~~an original~~ a watermark embedded into an original media data set, said first copy

control information required for determining at least whether ~~a copy of the~~ copying said original media data is permitted, wherein said ~~original~~ watermark further includes watermark type indicating whether the watermark is original or not and media owner identification information indicating a media owner;

an operation element performing an operation according to an analyzed result of said copy control information analyzer; and

a watermark generator embedding a device watermark into said performed media data set ~~when~~ and transferring said device watermark embedded media data set to an external device, said device watermark including a second copy control information ~~derived from the first copy control information~~ and the device identification information including model number and unique serial number.

11. (Currently Amended) The system of claim 10, wherein said device identification information is used to detect an origin of ~~the~~ said performed media ~~copy~~ data set, thereby performing a revocation of a compromised device or their key.

12. (Previously Presented) The system of claim 10, wherein said device identification information further includes device name.

13. (Canceled)

14. (Currently Amended) T he system of claim 10, wherein said media owner identification information is used to bind ~~the~~ said media owner with ~~the~~ said media data set.

15. (Canceled)

16. (Currently Amended) The method of claim 4, wherein said media owner identification information is used to bind ~~the~~ said media owner with ~~the~~ said media data set.

17. (New) The method of claim 1, wherein said second copy control information is set to "copy for display only" if said performed media data set is to be transferred to a displaying device, said "copy for display only" distinguishing a media data set for display only from said original media data set or a copied media data set for record.

18. (New) The system of claim 7, wherein said watermark generator embeds said device water mark including said second control information set to "copy for display only" if said performed media data set is to be transferred to a displaying device, said "copy for display only" distinguishing a media data set for display only from said original media data set or a copied media data set for record.